(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11341268 A**

(43) Date of publication of application: **10 . 12 . 99**

(51) Int. Cl **H04N 1/387**
H04N 7/24

(21) Application number: **11089986**

(22) Date of filing: **30 . 03 . 99**

(30) Priority: **30 . 03 . 98 US 98 52041**

(71) Applicant: **SEIKO EPSON CORP**

(72) Inventor: **BHASKARAN VASUDEV**
RATNAKAR VIRESH

(54) **METHOD FOR INSERTING WATERMARK TO DIGITAL IMAGE OR COMPRESSED DIGITAL IMAGE, DIGITAL IMAGE CAPTURING DEVICE, COMPUTER SYSTEM AND METHOD FOR DETECTING ALTERATION OF DIGITAL IMAGE WITH WATERMARK**

(57) Abstract:

PROBLEM TO BE SOLVED: To reduce distortion and to easily verify alteration by partially decoding digital images, generating plural data blocks, judging whether or not to bury watermark bits and burying the watermark bits in the data blocks.

SOLUTION: Images are partially decoded, plural blocks are generated and the quantization variable of the conversion coefficient of a highest frequency in the respective blocks is obtained and multiplied with the conversion coefficient. Whether or not to bury the watermark bit is judged based on the coefficient and the remaining watermark bit number of the watermark to be buried, the least significant bit of the conversion coefficient of the highest frequency of the block for which burying is decided is set to zero and a hash value calculated in the last block is turned to the hash value of the entire images. Then, by calculating the watermark from the hash value by using a secret key and digital signature algorithm, a ciphered hash value is obtained and the LSB of the conversion coefficient of the block to perform burying is matched with the watermark bit.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－341268

(43)公開日　平成11年(1999)12月10日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		
7/24		7/13	Ｚ	

審査請求　未請求　請求項の数21　ＯＬ　（全 13 頁）

(21)出願番号　特願平11－89986

(22)出願日　平成11年(1999) 3月30日

(31)優先権主張番号　０９／０５２，０４１

(32)優先日　1998年３月30日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号

(72)発明者　ヴァスデブ　バスカラン
アメリカ合衆国カリフォルニア州94043
マウンテンビュー　ノースウィスマンロード100

(72)発明者　ヴィレッシュ　ラトナカー
アメリカ合衆国カリフォルニア州サニーベイル　コルトマデラアベニュー970　アパートメント402

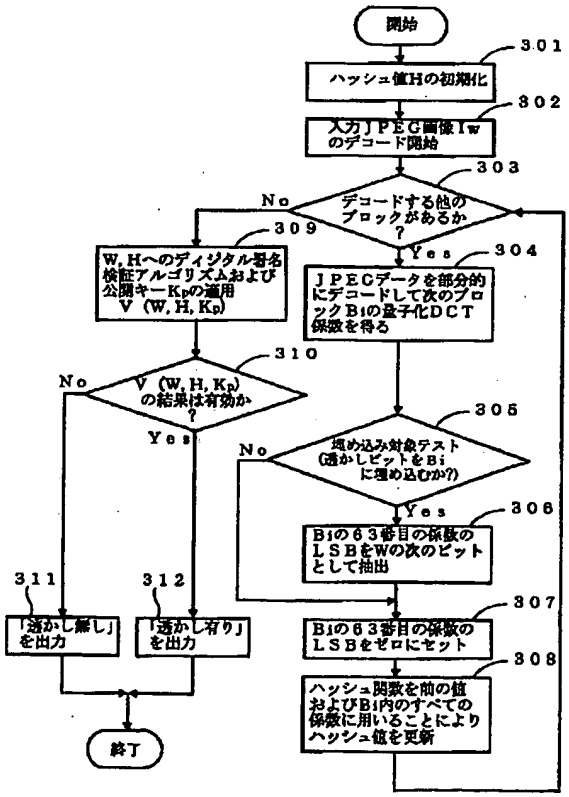
(74)代理人　弁理士　鈴木　喜三郎　（外２名）

(54)【発明の名称】　ディジタル画像または圧縮ディジタル画像への透かし挿入方法、ディジタル画像キャプチャリング装置、コンピュータシステム、および透かし入りディジタル画像の改ざん検出方法

(57)【要約】

【課題】　圧縮ディジタル画像の周波数ドメインにおいて脆弱な透かしを直接挿入または抽出する手法およびそのような透かし入りディジタル画像の改ざんの有無を測定する手法を提供する。

【解決手段】　透かしの挿入は、ディジタル画像の周波数関数にディジタル画像のハッシュ関数のディジタル署名のビットを埋め込むことで行う。改ざんの検出は、透かし挿入ステップの間に埋め込まれた脆弱透かしをディジタル画像から抽出し、ディジタル画像のハッシュ関数を挿入ステップと同様に計算し、公開キーを用いて、抽出した透かしがハッシュ値の有効署名であるか否かを検証することで行う。有効であれば、そのディジタル画像は改ざんされていないことになり、有効でなければ、そのディジタル画像が改ざんされたことになる。



【特許請求の範囲】

【請求項１】　ディジタル画像に透かしを挿入する方法において、

圧縮ディジタル画像を部分的にデコードして、それぞれが複数の変換係数を有してなる複数のデータブロックを生成するステップ、

前記各データブロックの複数の変換係数の一係数およびディジタル画像に埋め込むべき透かしの残り透かしビット数に基づき、当該データブロックに透かしビットを埋め込むか否かを判断するステップ、

ディジタル署名アルゴリズムおよびシークレットキーを用いて、複数のビットを有する透かしをディジタル画像全体について計算するステップ、および、

前記した各データブロックの複数の変換係数の一係数に、前記の計算した透かしの対応するビットをマッチさせるようにセットすることにより、透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしを埋め込むべく判断された各データブロックに、透かしビットを埋め込むステップ、を含むことを特徴とするディジタル画像への透かし挿入方法。

【請求項２】　前記した各データブロックの複数の変換係数の一係数が、当該データブロックの最高周波数を表わす変換係数であることを特徴とする請求項１に記載の圧縮ディジタル画像への透かし挿入方法。

【請求項３】　透かしを計算する前記ステップが、透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしを埋め込むべきと判断された各データブロックの、複数の変換係数の一係数の少なくとも１ビットをゼロにセットするステップをさらに含んでなることを特徴とする請求項１または２に記載の圧縮ディジタル画像への透かし挿入方法。

【請求項４】　透かしを埋め込む前記ステップが実行された後に、部分的にデコードされた前記複数のデータブロックをエンコードして、透かし入りディジタル画像を再圧縮するステップをさらに含んでなることを特徴とする請求項１～３の何れかに記載の圧縮ディジタル画像への透かし挿入方法。

【請求項５】　透かしを計算する前記ステップが、各データブロックについてハッシュ関数を用いることにより各データブロックでハッシュ値を更新するステップをさらに含み、最後のデータブロックについて計算されたハッシュ値がディジタル画像全体を表わす多重ビットのハッシュ値であることを特徴とする請求項１～４の何れかに記載の圧縮ディジタル画像への透かし挿入方法。

【請求項６】　透かしを計算する前記ステップが、各データブロックの複数の変換係数の一係数の量子化変数を得るステップ、および各データブロックの変換係数の一係数を前記量子化変数と掛け合わせるステップをさらに含んでなる請求項１～５の何れかに記載の圧縮ディジタル画像への透かし挿入方法。

【請求項７】　ディジタル画像に透かしを挿入する方法において、

複数ビットを有する透かしをディジタル画像全体について計算するステップを有し、当該ステップが、

圧縮ディジタル画像を部分的にデコードして、それぞれが複数の変換係数を有してなる複数のデータブロックを生成するステップ、

各データブロックの複数の変換係数の一係数について量子化変数を得るステップ、

前記の各データブロックの複数の変換係数の一係数を、前記量子化変数と掛け合わせるステップ、

前記各データブロックの最高周波数を表す、当該データブロックの複数の変換係数の一係数およびディジタル画像に埋め込むべき透かしの残り透かしビット数に基づき、各当該データブロックに透かしビットを埋め込むか否かを判断するステップ、

透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしを埋め込むべく判断された各データブロックの複数の変換係数の一係数の少なくとも１ビットをゼロにセットするステップ、

各データブロックについてハッシュ関数を用いることにより各データブロックについてハッシュ値を更新し、最後のデータブロックにおいて計算されたハッシュ値がディジタル画像全体を表わす多重ビットのハッシュ値となるステップ、およびシークレットキーおよびディジタル署名アルゴリズムを多重ビットのハッシュ値に用いて透かしを計算するステップ、を含み、さらに、

当該データブロックの複数の変換係数の一係数の少なくとも１ビットに、前記計算された透かしの対応するビットをマッチさせるようにセットすることにより、透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしを埋め込むべきと判断された各データブロックに、透かしビットを埋め込むステップを有する、ことを特徴とする圧縮ディジタル画像への透かし挿入方法。

【請求項８】　透かし入りディジタル画像の改ざんを検出する方法において、

圧縮した透かし入りディジタル画像を部分的にデコードして、それぞれが複数の変換係数を有してなる複数のデータブロックを生成するステップ、

透かしビットが埋め込まれるデータブロックを判断するステップ、

透かしビットが埋め込まれるデータブロックを判断する前記ステップにおいて透かしビットの埋め込み対象であると判断した各データブロックから、当該データブロックの複数の変換係数の一係数から少なくとも１ビットを抽出して抽出透かしを生成するステップ、

最後のデータブロックについて計算されたハッシュ値がディジタル画像全体を表わす多重ビット値であり、当該データブロックの複数の変換係数の一係数の少なくとも１ビットのゼロ化された値に基づいて、各データブロックについてハッシュ関数を用いることにより、ディジタル画像のハッシュ値を計算するステップ、および、

抽出された透かしおよび多重ビットで計算されたハッシュ値ならびに公開キーに、ディジタル署名アルゴリズムを用いて、圧縮ディジタル画像が改ざんされたか否かを判断するステップ、

含むことを特徴とする圧縮ディジタル画像~~への透かし挿入~~方法。

【請求項９】　各データブロックの複数の変換係数の一係数が、当該データブロックの最高周波数を表わす変換係数である請求項８に記載の圧縮ディジタル画像への透かし挿入方法。
【請求項１０】　光をキャプチャリングし、その光をアナログディジタル画像信号に変換するセンサと、
アナログディジタル画像信号をディジタル画像信号に変換するアナログ－ディジタル変換器と、
ディジタル画像を圧縮して、それぞれが複数の変換係数を有する複数のデータブロックを生成し、当該データブロックの複数の変換係数の一係数およびディジタル画像に埋め込まれるべき透かしの残り透かしビット数に基づいて、各データブロックに透かしビットを埋め込むか否かを判断し、複数のビットを有する透かしをディジタル画像全体について計算し、当該データブロックの複数の変換係数の一係数に、前記の計算した透かしの対応するビットをマッチさせるようにセットすることにより、透かしを埋め込むべく判断された各データブロックに、透かしビットを埋め込むディジタル画像プロセッサと、からなるディジタル画像キャプチャリング装置。
【請求項１１】　前記のディジタル画像プロセッサが、透かしビットを埋め込むべく判断された各データブロックの複数の変換係数の一係数の少なくとも１ビットをゼロにセットしてなる請求項１０に記載のディジタル画像キャプチャリング装置。
【請求項１２】　前記のディジタル画像プロセッサが、透かしビットの埋め込みを完了した後に、透かしが埋め込まれた複数のデータブロックをエンコードして透かし入りディジタル画像を再圧縮してなる請求項１０または１１に記載のディジタル画像キャプチャリング装置。
【請求項１３】　前記のディジタル画像プロセッサが、各データブロックについてハッシュ関数を用いることにより各データブロックについてハッシュ値を更新するものであって、最後のデータブロックで計算されたハッシュ値がディジタル画像全体を表わす多重ビットのハッシュ値であることを特徴とする請求項１０～１２の何れかに記載のディジタル画像キャプチャリング装置。
【請求項１４】　前記のディジタル画像プロセッサが、各データブロックの複数の変換係数の一係数の量子化変数を取得し、当該ブロックデータブロックの複数の変換係数の一係数を、前記量子化変数と掛け合わせることを特徴とする請求項１０～１３の何れかに記載のディジタル画像キャプチャリング装置。
【請求項１５】　プロセッサが、圧縮透かし入りディジタル画像の改ざんを検出するように組み込まれたコンピュータ可読プログラムコードを有する、プロセッサおよびメモリを含むコンピュータシステムにおいて、
圧縮した透かし入りディジタル画像を部分的にデコードして、各それぞれが複数の変換係数を有してなる複数のデータデータブロックを生成するステップ、
透かしビットが埋め込まれるべきデータブロックを判断するステップ、
透かしビットが埋め込まれるべきデータブロックを判断する前記ステップにおいて透かしビットの埋め込み対象であると判断された各データブロックから、当該データブロックの複数の変換係数の一係数のうち、少なくとも１ビットを抽出して、抽出された透かしを生成するステップ、
最後のデータブロックで計算されたハッシュ値がディジタル画像全体を表わす多重ビット値である、当該データブロックの複数の変換係数の一係数の少なくとも１ビットのゼロ化された値に基づいて、各データブロックについてハッシュ関数を用いることにより、ディジタル画像のハッシュ値を計算するステップ、および、
ディジタル署名アルゴリズムを用いることにより、抽出された透かしと多重ビット値とを比較して、圧縮透かし入りディジタル画像が改ざんされたか否かを判断するステップ、を実行することを特徴とするコンピュータシステム。
【請求項１６】　各データブロックの複数の変換係数の一係数が当該データブロックでの最高周波数を表わす変換係数であることを特徴とする請求項１５に記載のコンピュータシステム。
【請求項１７】　複数の画素を有するディジタル画像に透かしを挿入する方法において、
複数のビットを有する透かしをディジタル画像全体について計算するステップを有し、当該ステップが、
当該画素を表わす複数のビットの一つおよびディジタル画像に埋め込むべき透かしの残留透かしビット数に基づき、各データブロックに透かしビットを埋め込むか否かを判断するステップ、
透かしビットを埋め込むべく判断する前記の判断ステップで判断される各画素の少なくとも一つのビットをゼロにセットするステップ、
ハッシュ関数を用いることにより各画素でハッシュ値を更新するステップであって、最後の画素で計算されたハッシュ値がディジタル画像全体を表わす多重ビットのハッシュ値であるステップ、および、
シークレットキーおよびディジタル署名アルゴリズムを多重ビットのハッシュ値に用いて透かしを計算するステップを含み、
かつ、
当該画素の少なくとも１ビットに、計算された透かしの対応するビットをマッチさせるようにセットすることにより、透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしを埋め込むべく判断された各画素に、透かしビットを埋め込むステップ、を含むことを特徴とするディジタル画像への透かし挿入方法。
【請求項１８】　少なくとも一つのビットは最小有効ビットである請求項１７に記載のディジタル画像への透かし挿入方法。
【請求項１９】　複数の画素を有する透かし入りディジタル画像の改ざんを検出する方法において、
透かしビットが埋め込まれる各画素を判断するステップ、
前記の判断ステップで透かしビットの埋め込み対象であると判断した各画素から、当該画素を表わす複数のビットの少なくとも１ビットを抽出して、抽出透かしを生成するステップ、

最後の画素について計算されたハッシュ値がディジタル画像全体を表わす多重ビット値であり、当該画素のビットの少なくとも１ビットのゼロ化された値に基づいて、各画素についてハッシュ関数を用いることにより、ディジタル画像のハッシュ値を計算するステップ、および、抽出された透かしおよび多重ビットで計算されたハッシュ値ならびに公開キーにディジタル署名検証アルゴリズムを用いて、圧縮ディジタル画像が改ざんされたか否かを判断するステップ、を含むことを特徴とする透かし入りディジタル画像の改ざん検出方法。

【請求項２０】　少なくとも１ビットは最小有効ビットである請求項１９に記載のディジタル画像の改ざん検出方法。

【請求項２１】　圧縮ディジタル画像に透かしを挿入する方法において、

目視可能な透かしを加えるステップ、

ディジタル画像および目視可能な透かしから目視不可能な透かしを計算するステップを有し、当該ステップは、

圧縮ディジタル画像を一部デコードして、各データデータブロックが複数の変換係数を有する複数のデータデータブロックを生成するステップ、

各データブロックの複数の変換係数の一係数の量子化変数を取得するステップ、

各データブロックの複数の変換係数の一係数を量子化変数と掛け合わせるステップ、

当該データブロックの最高周波数を表す、当該データブロックの複数の変換係数の一係数およびディジタル画像ディジタル画像に埋め込むべき透かしの残り透かしビット数に基づき、各データブロックに透かしビットを埋め込むか否かを判断するステップ、

目視可能な透かしビットを埋め込むべく判断する前記ステップにおいて判断される各データブロックの複数の変換係数の一係数の少なくとも１ビットをゼロにセットするステップ、

ハッシュ関数を用いることにより各データブロックでハッシュ値を更新するステップであって、最後のデータブロックで計算されたハッシュ値がディジタル画像全体を表わす多重ビットのハッシュ値であるステップ、および、

シークレットキーおよびディジタル署名アルゴリズムを多重ビットのハッシュ値に用いて目視可能な透かしを計算するステップ、を含み、

かつ、

当該データブロックの複数の変換係数の一係数の少なくとも１ビットに、前記計算された目視可能な透かしの対応するビットをマッチさせるようにセットすることにより、データブロックに透かしビットを埋め込むか否かを判断する前記ステップにおいて、透かしを埋め込むべく判断された各データブロックに目視可能な透かしビットを埋め込むステップ、を有することを特徴とする圧縮ディジタル画像への透かし挿入方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、一般には脆弱透かし挿入技術に関し、さらに詳しくは圧縮ディジタル画像の周波数ドメインにおいて脆弱な透かしを直接挿入あるいは抽出する技術およびそのような透かし入りディジタル画像の改ざんがなされたか否かを測定する技術に関する。

【０００２】

【従来の技術】透かし（ウォーターマーク）とはディジタル画像のようなディジタル創作物に埋め込まれたディジタルパターンである。ディジタル画像に透かしを挿入する処理は、圧縮ディジタル画像で典型的に用いられる、周波数ドメイン（周波数領域）表現において直接行うことができる。

【０００３】透かしは、歪みの発生を最小限に抑えつつ、ある周波数係数を変更することによって挿入することができる。ＪＰＥＧディジタル画像圧縮標準で用いられているような、ブロック基準の周波数ドメイン表現の場合、周波数とともにブロックも変更の対象として選ぶことにより歪みを少なくすることができる。いずれの場合も透かしがディジタル画像に挿入された後でその透かしを有効なものとするには、典型的には、ある種のソフトウェアを用いてインプリメントする手順が必要とされる。

【０００４】透かしには異なる種類があり、異なった目的で用いられる。例えば、改ざんに耐える透かしは、ディジタル画像の所有権者または特定受権者を同定するように設計されている。同定手段として有効に透かしを機能させる（すなわち、ディジタル画像の不正な頒布をトレースあるいは追跡する）ためには、ディジタル画像を視覚的に傷つけずには透かしを取り除くことが不可能となるか、または少なくとも困難にするようにして、改ざんに耐える透かしをディジタル画像に埋め込まねばならない。また、このような透かしは、ディジタル画像処理技術、例えばクロッピング、スケーリング、ディジタル画像のエンハンスメント、圧縮／伸張（コンプレス／デコンプレス）等にも耐えるものでなければならない。さらに、改ざんに耐える透かしは、何者かがディジタル画像を改ざんしたとしても、正当な所有権者が容易に検出、再生して、ディジタル画像の頒布をトレースし、ディジタル画像を同定できるようにすべきである。

【０００５】別の種類の透かしは脆弱透かしとも呼ばれ、ディジタル画像の改ざんを検出するために設計されている。脆弱透かしは、もし誰かがディジタル画像を改ざんすれば、その改ざんにより透かしが変更または破壊されるように埋め込まれている。脆弱透かしは、例えば、ディジタルカメラで生成したディジタル画像との関連では、ディジタル画像が作られた後に改ざんしたか否かを判断する基準を設けるのに用いることができる。

【０００６】これまでに多くの透かし挿入法が提案されている。例えば、米国特許第５，５３０，７５９号明細書には、線形カラー空間内の原ディジタル画像の画素サンプル値に対する多重修正として、その原ディジタル画像にディジタル透かしを用いて、画素の色度が変えられないようにすることが提案されている。この手順により、単純に原ディジタル画像に加えられた目に見える透かしが得られる。

【０００７】米国特許第５，６０６，６０９号明細書には

電子ドキュメント確認システムおよび方法が記載されている。この特許はドキュメントに電子的に署名することを扱っているが、その署名はドキュメントデータ自体に埋め込まれるものではない（すなわち、ドキュメントデータは変更されない）。署名は別のフィールドとしてドキュメントに単に加えられるだけである。

【０００８】米国特許第５，６１３，００４号および５，６８７，２３６号明細書は、ステガノグラフィー（一目瞭然ではない情報の隠蔽）および暗号法（セキュリティーなしの手段で送られる情報のスクランブリング）を統合したものである。データに透かしを入れておき、もしそれがコピーされた場合には、オリジナルの所有者を判定することができる。したがって、これらの特許の透かし挿入方式は改ざんに耐える得る形式である。

【０００９】米国特許第５，６６４，０１８号明細書では、デジタイズされた画像のコピーの各セットが、わずかに修正された形の「ベースライン」透かしを有する、透かし挿入法が提案されており、「ベースライン」透かしは、データのあるクリティカル領域内に位置する。この方法は改ざんに耐える方式に属するものであって、単一ディジタル画像の異なる透かし入りコピーを有する複数の者が共同して透かしを除こうとしても、内容を壊さずに透かしを除きにくくしてある。

【００１０】米国特許第５，６８９，５８７号明細書には、ディジタル画像内のデータを隠蔽する方法および装置について記載されている。この特許はディジタル画像内の情報を隠蔽する方法であって、改ざんへの対抗（著作権型の保護）を保証するものである。

【００１１】

【発明が解決しようとする課題】しかし、いずれの特許も改ざんを検出するための脆弱透かし方式を提供するものではない。さらに、いずれの特許も、ディジタル画像の周波数ドメイン表現内に直接インプリメントして、埋め込んだ透かしに起因する歪みを最小限に止める透かし挿入技術を提供するものではない。しかも、これらの特許のその他の欠点は、圧縮ディジタル画像の完全な伸張を必須とせずには挿入および検証の手順を行い得ない点である。

【００１２】したがって、本発明の目的は上述の問題を克服することである。

【００１３】本発明の他の目的は、周波数ドメインにおいて脆弱透かしを挿入および抽出し、また透かしを挿入したディジタル画像が改ざんを受けたか否かを検証するための方式を提供することである。

【００１４】本発明のさらに他の目的は、ディジタル画像のための脆弱透かし挿入方式との関連で検証の手順を提供することにあり、もし改ざんが発生した場合には、当該検証の手順が、壊された透かしを明らかにし、かつそのディジタル画像の改ざんの発生を知らせる基準を設けるようにすることである。

【００１５】本発明のさらに他の目的は、シークレットキーを挿入ステップでのみ用い、他方、検証は公開キーを用いて行う、周波数ドメインでの透かしの挿入および検証法を提供することである。

【００１６】本発明のさらに他の目的は、圧縮ディジタル画像の完全伸張を必要としない透かし挿入および検証法を提供することである。

【００１７】

【課題を解決するための手段】本発明の一態様によれば、ディジタル画像に脆弱透かしを埋め込む技術、およびこのようにして透かしを入れたディジタル画像の改ざんを検出する技術が提供される。

【００１８】本発明の別の態様には、圧縮ディジタル画像を完全に伸張することなく当該圧縮ディジタル画像に透かしを入れ、また、このようにして透かしを入れた圧縮ディジタル画像の改ざんを検出することが含まれる。

【００１９】本発明のさらに別の態様には、挿入メカニズムではシークレットキーを用い、対応する検証メカニズムでは公開キーを用いるものが含まれる。

【００２０】圧縮ディジタル画像への透かし挿入には、最初にそのディジタル画像についてハッシュ値を計算することが含まれるが、この計算は次のようにして行われる。すなわち、圧縮ディジタル画像を部分的にデコードして、それぞれが複数の変換係数を有する複数のブロックを生成する。各ブロックの中で最高周波数の変換係数についての量子化変数を得て、前記変換係数と前記量子化変数を掛け合わせる。つぎに、各ブロックにおける最高周波数の係数、およびディジタル画像に埋め込まれるべき透かしの残り透かしビット数に基づいて、ブロックに透かしビットを埋め込むか否かを判断する。そして透かしビットを埋め込むと決まったブロックの最高周波数の変換係数の最下位ビット（ＬＳＢ）をゼロにセットし、各ブロックについてハッシュ関数を用いてハッシュ値を更新する。ここで、最後のブロックで計算したハッシュ値は、ディジタル画像全体のハッシュ値を表わす多重ビット値である。

【００２１】ディジタル画像全体についてのハッシュ値が計算されると、シークレットキーおよびディジタル署名アルゴリズムを用いて、計算済みのハッシュ値から透かしが計算される。すなわち、暗号化されたハッシュ値が求められる。

【００２２】次いで、先に透かしの埋め込みを行うべきと判断されたブロックにおける最高周波数の変換係数のＬＳＢを、対応する透かしビットにマッチさせるようにセットする。これにより、透かしの埋め込みを行うべきブロックに透かしビットが埋め込まれる。

【００２３】そして、透かしを埋め込んだディジタル画像が改ざんされたか否かを判断するために以下のステップが行われる。

【００２４】すなわち、透かしを埋め込んだ圧縮ディジタル画像を部分的にデコードして、それぞれが複数の変換係数を有する複数のブロックを生成する。

【００２５】そして、透かしビットが埋め込まれている各ブロックを判断する。つぎに、透かしビットが埋め込まれたものとして予め判断された各ブロックから、そのデータブロックにおける最高周波数の係数のＬＳＢを抽出して抽出透かしを生成する。ＬＳＢがゼロにセットされたデータブロックにおける最高周波数の変換係数の値に基づき、各データブロックでのハッシュ関数を適用することにより、ディジタル画像のハッシュ値を計算し（なお、

このデータブロックでは最後のデータブロックで計算したハッシュ値がディジタル画像全体を表わす多重ビット値である)、抽出された透かしおよび計算されたハッシュ値にディジタル署名アルゴリズムを適用し、かつ公開キーを用いて、透かしを入れた圧縮ディジタル画像が改ざんされたか否かを判断する。

【００２６】透かし挿入の手順はディジタルカメラのようなディジタル画像キャプチャー装置内で直接行うこともできるし、または適当な構成のコンピュータで行うこともできる。また、このようなコンピュータは、透かし入りのディジタル画像を調べて改ざんが加えられたか否かを判断し、もし改ざんが加えられていれば当該画像が存在している場所を決定するのにも用いることができる。

【００２７】添付の図面とともに以下の説明および特許請求の範囲により、本発明の上述した以外の目的および内容について十分な理解を得ることができる。

【００２８】

【発明の実施の形態】ディジタル画像周波数ドメインにおいてディジタル画像に透かしを挿入するため、ディジタル画像を一旦走査して、そのディジタル画像のｋビットのハッシュ値を表わすＨを計算する。そして、ディジタル署名アルゴリズムＳおよびシークレットキーＫＳを用いてｍビットの透かしＷ＝Ｓ（Ｈ，ＫＳ）を計算する。次いで、ディジタル画像への透かし挿入手順の二次パスを用いて、ディジタル画像に透かしＷが埋め込まれる。これらのステップを図１，図２，図３に示す。

【００２９】先ず図２を参照し、次いで図１および図３を参照すると、ステップ１０１では初期の走査手順でハッシュ値Ｈが固定値に初期化される。ステップ１０２では、ＪＰＥＧ画像Ｉの形態の圧縮ディジタル画像がデコーダに送られる。デコーダは、ＪＰＥＧデータからヘッダを分析し、最高周波数の係数についての量子化テーブルエントリーであるｑの値を知ることができる。この最高周波数の係数は、ＪＰＥＧで用いられる８×８離散コサイン変換（ＤＣＴ）についての６３番目の係数である。

【００３０】もし、さらにデコードおよび処理（ステップ１０３）されるべき他のデータブロック（次のデータブロック）があれば、当該次のデータブロックＢｉはステップ１０４で部分的にデコードされる。圧縮データのエントロピー符号化は行われずに、完全伸張に必要とされるデ・ジグザグ（ｄｅ－ｚｉｇ－ｚａｇｇｉｎｇ）化、非量子化（ｄｅｑｕａｎｔｉｚａｔｉｏｎ）および逆離散コサイン変換（ＩＤＣＴ）のステップが回避される。そして、ジグザグ順に配置した非ゼロ量子化係数のみからなるデータブロックＢｉの表現が得られる。

【００３１】本発明では、６３番目の変換係数を特別に透かし挿入に用いているので、その値がゼロであってもデータブロックＢｉの表現は常に６３番目の変換係数を有する構成となる。すなわち、データブロックＢｉの表現には常に６３番目の係数が情報として含まれる。このようにして、他の非ゼロ量子化係数も、デ・ジグザグ化なしに容易に行うことができることに注意すべきである。なぜなら、６３番目の変換係数がジグザグ順の最後の係数であるからである。

【００３２】次いでデータブロックＢｉのデコードされた表現は、ステップ１０５に渡され、その６３番目の変換係数と量子化変数ｑ（ステップ１０２で得られる）とが掛け合わされる。

【００３３】このステップが行われる理由は以下の通りである。より高い周波数における小さな変動は肉眼では判断できない。歪みを最小限に止めるため、透かしＷは最高周波数の係数（この場合６３番目の係数）のみを変更することによってビット単位で埋め込まれる。

【００３４】透かしビットに等しい値に、前記の６３番目の変換係数のＬＳＢを変えることにより、透かしビットが係数値に埋め込まれる(後述の図３のステップ２０７)。６３番目の係数の値がｖであれば、このＬＳＢの変動により、プラスまたはマイナスｑ（ここでｑは６３番目の変換係数の量子化変数である）で非量子化された係数が変動する。この変動を最小にするため、本実施例では６３番目の変換係数の量子化変数ｑを１にセットし、各データブロックにおける６３番目の変換係数（埋め込み中の透かしビットではない）を非量子化値（ｑとの掛け合わせで得られる）と直接置き換える。

【００３５】このステップにより、伸張の際の歪みは、プラスまたはマイナス１のみである。６３番目の変換係数はほとんどのデータブロックで典型的には、もともとゼロであり、非ゼロ係数のみが圧縮サイズの大半についてあるので、ステップ１０５での掛け合わせによって生じる圧縮サイズの増加は最小限となる。

【００３６】ステップ１０６では透かしビットをデータブロックＢｉに埋め込むべきか否かの決定がなされる。ステップ１０６での決定の手順は、ディジタル画像に生じる歪みを最小にするとともに、圧縮ディジタル画像のサイズ増も最小にするように設計される。この決定手順は後述の二箇所で再度用いられるので、単に埋め込み対象テスト（ＥＭＢＥＤＤＥＲ－ＴＥＳＴ）と呼ぶ。以下、埋め込み対象テストについて詳述する。

【００３７】カラーディジタル画像については、透かしはディジタル画像の輝度面にのみ埋め込まれる。この埋め込みは、伸張される間に輝度－色度カラー表示が赤、緑および青の画素値（ＲＧＢ）に変換されるとき、発生する歪みを最小にするように行われる。さらに、色度面は典型的には準サンプル化されており、したがって単一の色度データブロックにおけるいかなる歪みも数個のＲＧＢデータブロックに歪みを生じる。このため、グレースケールディジタル画像およびカラーディジタル画像では、透かしビットはゼロ付番されたカラー成分（カラーディジタル画像用の輝度面）のみに埋め込まれる。

【００３８】前述の通り、歪みを最小にするために透かしビットは６３番目のＤＣＴ係数にのみ埋め込まれる。圧縮サイズを最小にするために、６３番目のＤＣＴ係数がすでに非ゼロであるデータブロックのみを選んで、透かしビットを埋め込む。このことは、ゼロ値から非ゼロ値への変化が、非ゼロ値から他のゼロ値への変化に比して、はるかに大きな圧縮サイズのもたらす観察結果に従うものである。

【００３９】埋め込み対象テストは透かし検証手順によっ

ても行われる。しかし、６３番目の係数（非量子化）がプラス１またはマイナス１であるデータブロックでも埋め込み対象としては選ばない。何故なら、透かしビットを埋め込む際にゼロに戻り、そのため検証部が、埋め込まれたデータブロックを決定できなくなるなるためである。

【００４０】埋め込み用に残っている透かしビットの数が、ある時点で、残りのデータブロック数に等しくなれば、残りの各データブロックは透かしビットの埋め込み対象として決定される。

【００４１】データブロックＢｉに透かしビットを埋め込む決定が「ＹＥＳ」であれば、６３番目のＤＣＴ係数のＬＳＢは、ステップ１０７でゼロにセットされて、その手順がステップ１０８に進む。決定が「ＮＯ」であれば、この手順は直接ステップ１０８に進む。ハッシュ値Ｈはその前の値を用いてステップ１０８で更新され、そしてジグザグ順に配置した、データブロックＢｉにおけるすべての非ゼロ量子化係数値は、一方向ハッシュ関数を用いることにより更新される。６３番目の係数はゼロであっても常にこのハッシュ値の計算に含まれる。

【００４２】すべてのデータブロックが処理されると、手順はステップ１０９に進み、計算されたハッシュ値ＨおよびシークレットキーＫＳにディジタル署名アルゴリズムＳが適用されてｍビットの透かしＷ＝Ｓ（Ｈ，ＫＳ）を計算する。

【００４３】先ず、図３を参照し、次いで図１および２を参照すると、透かし挿入手順の二次パスでは、入力ＪＰＥＧディジタル画像Ｉが再びデコーダに送られるが、デコーダは、ステップ２０１で６３番目のＤＣＴ係数についての量子化変数であるｑ値を符号化するヘッダを分析する。

【００４４】ステップ２０２では、透かし入り出力ＪＰＥＧディジタル画像についてのヘッダＩＷが入力ディジタル画像からの直接コピーによって生成される。ただし、量子化テーブルにおける６３番目のＤＣＴ係数の量子化変数は、その前の値ｑの代わりに１に変えられる。さらにデコードされ、処理（ステップ２０３）されるべき他のデータブロックがあれば、その次のデータブロックＢｉはステップ２０４で部分的にデコードされる。前述したと同様に、圧縮画像データのエントロピー符号化は行われず、完全伸張に必要なデ・ジグザグ化、非量子化およびＩＤＣＴのステップが回避される。その結果、非ゼロ量子化係数のみからなるＢｉの表現（ただし、常に当該表現に含まれる６３番目の係数については除く）がジグザグ順の配置を伴って生じる。

【００４５】ステップ２０５では、各データブロックの６３番目のＤＣＴ係数と量子化変数ｑとが掛け合わされる。埋め込み対象テストがステップ２０６で行われ、データブロックＢｉにＷの次のビットを埋め込むか否かを判断する。この判断はデータブロック毎に再び行ってもよく、これらの結果がメモリに記憶されれば、前の決定を下すステップ（ステップ１０５）を用いて行ってもよい。いずれの場合も、データブロックＢｉにＷの次のビットを埋め込むことになれば、ステップ２０７においてＢｉの６３番目のＤＣＴ係数のＬＳＢはＷの次のビットにマッチするようにセットされ、そして手順は次のステップ２０８に進む。ステップ２０６の決定が「ＮＯ」であれば、手順は直接ステップ２０８に進む。

【００４６】ステップ２０８では、データブロックＢｉにおけるＤＣＴ係数がエンコードされ、透かし入りディジタル画像Ｉｗについての圧縮データストリームへの出力として生成される。量子化係数はすでにジグザグ順になっているので、ここで用いるデータブロックＢｉの量子化係数の表現により、有効なエンコードが可能となり、そのため一般に圧縮に必要なＤＣＴ、量子化およびジグザグ化のステップが回避される。このステップはすべてのデータブロックが処理されるまで繰り返される。

【００４７】周波数ドメイン透かし挿入法の検証手順を図４および図５に示す。この手順はディジタル画像が改ざんされたか否かを判断するために用いられる。

【００４８】図５では、ステップ３０１でハッシュ値Ｈが初期化された後、ステップ３０２では透かし検証手順が起動して入力ディジタル画像Ｉｗをデコードし、ヘッダを分析する。ステップ３０３では、デコードすべきデータブロックが他に残っているか否かを判断する。もし残っていれば、ステップ３０４で次のデータブロックＢｉが部分的にデコードされる。ここで再び、圧縮データのエントロピー符号化は行われず、完全伸張に必要なデ・ジグザグ化、非量子化およびＩＤＣＴのステップが回避される。この結果、非ゼロ量子化係数のみからなるデータブロックＢｉの表現（ただし、常に当該表現に含まれる６３番目のＤＣＴ係数については除く）がジグザグ順の配置を伴って生じる。埋め込み対象テストはステップ３０５で行われ、データブロックＢｉに透かしＷの次のビットを埋め込むか否かを判断する。

【００４９】透かしＷを埋め込むべきと判断されると、ステップ３０６においてデータブロックＢｉの６３番目のＬＳＢは透かしＷの次のビットとして抽出され、ステップ３０７でそのＬＳＢがゼロにセットされる。データブロックＢｉが透かしビットの埋め込み対象でないときは、手順はステップ３０７およびステップ３０５からステップ３０８に移行する。ハッシュ値Ｈはその前の値を用いることによりステップ３０８で更新され、またデータブロックＢｉにおける非ゼロ量子化係数のすべての値は、ジグザグ順の配置とともに、一方向ハッシュ関数を用いることにより更新される。６３番目のＤＣＴ係数はゼロであっても常にこのハッシュ値の計算に含まれる。このステップはすべてのブロックを通して継続し、そして最後に抽出された透かしＷおよびハッシュ値Ｈが完全に計算される。

【００５０】この時点で、公開キーＫｐ（シークレットキーＫＳに対応）を用いて、ディジタル署名アルゴリズムＶ（署名アルゴリズムＳに対応）に適用され、ステップ３０９で透かしＷがＳ（Ｈ，ＫＳ）と同じか否かを検証する。ステップ３０９はシークレットキーＫＳの使用を必要としない点に注意すべきである。ステップ３１０では、ステップ３０９で適用されたディジタル署名検証アルゴリズムＶ（Ｗ，Ｈ，Ｋｐ）の出力が調べられる。もし、アルゴリズムＶ（Ｗ，Ｈ，Ｋｐ）が合格であれば、ディジタル

画像は完全な脆弱透かしを有しており、したがって改ざんされていないことになる（ステップ３１２）。もし、アルゴリズムＶ（Ｗ，Ｈ，Ｋｐ）が不合格であれば、脆弱透かしは（まだ存在しているとして）すでに破壊されており、したがってディジタル画像は改ざんされたか、キーの対（ＫＳ，Ｋｐ）に対応する脆弱透かしを有していなかったと結論できる（ステップ３１１）。

【００５１】ディジタル画像改ざん検証ステップの効果はハッシュ関数の強さと署名および検証アルゴリズムＳおよびＶに左右される。種々の一方向ハッシュ関数を用いることができるが、例えば、アール・リベスト（Ｒ．Ｒｉｖｅｓｔ）が開発したＭＤ５と呼ばれるハッシュ関数、あるいはＳＨＡまたはＲＩＰＥＭＤハッシュ関数がある。同様に、署名および検証アルゴリズムに用い得るものも数多くあり、例えばエルガマル（Ｅｌ　Ｇａｍａｌ）スキーム、ＤＳＡアルゴリズムまたはＲＳＡアルゴリズムがある。

【００５２】この脆弱透かし挿入手順を変更して、改ざんがすでになされたディジタル画像の領域を大まかに調べることができる。この方法は、ディジタル画像を数個の領域に区分し、各領域に別々にすべての挿入手順を施すことによって行うなわれる。改ざんされた箇所を含む領域のみが透かしの破壊を示す。しかし、この変更された手順では制限された形式の改ざんは検出されない。なお、このような改ざんは、異なるディジタル画像から抽出した数領域のコラージュまたは単一ディジタル画像からの再配列領域（各領域は有効な透かしをもたらしている）のコラージュであるディジタル画像を形成させることによって行われるものである。しかし、このような改ざんはその領域が十分大きければ一目瞭然である。

【００５３】同様な脆弱透かし挿入法は空間領域にも応用することができる。最高周波数の係数の代わりに、すべての画素またはその一部を透かしビット埋め込み対象として直接用い、ハッシュ関数の計算に先だってＬＳＢをゼロにセットし、次いでこのＬＳＢを二次パスにおける透かしビットにセットすることによって行う。本発明は空間および周波数ドメインの透かし挿入法の統合に限定されるものではない。また、本発明は、上述したような透かしの挿入を周波数ドメイン内で行い得るようにし、一方、対応する透かしの検証を上述の通り空間領域内で行うことに限定されるものではない。

【００５４】さらに、この透かしは目視可能な透かしとすることができる。特有の透かし信号の変換周波数係数を計算し、これをディジタル画像の係数に単純に追加することにより、目視可能な透かしを周波数ドメインに埋め込むことができる。このステップはディジタル画像のコード化（例えばＤＣＴ）で共通に用いられる変換の直線性の結果としての作用をするが、画素領域内でのこのような追加が周波数ドメインでの追加に対応することを保証するものである。同様な目視可能な透かし挿入法は空間領域でも行うことができる。

【００５５】本発明の透かし挿入、抽出および検証手順を説明するブロック図および流れ図は、ある特定な機能の実行および関連性を説明するものである点に注意すべきである。これらの機能的ブロックの境界は説明の都合で任意に限定したものである。特定な機能および関連性が適当に得られる限りにおいて、この境界に代わるものを定めることができる。さらに、この流れ図は、シンタックスまたはいかなる特定のプログラム言語を表わすものではない。むしろこれらの図は、当業者が必要な処理を行うための回路を組み立て、またはソフトウェアを作成するのに必要な機能上の情報を示すものである。ブロック図および流れ図に示す各機能は、例えば、ソフトウェアの命令、ディジタル信号処理回路のような機能的に等しい回路、アプリケーションスペシフィック集積回路（ＡＳＩＣ）またはこれらの組合せによってインプリメントされる。

【００５６】本発明の透かし挿入法は、そのブロック図を図６に示すディジタルカメラを含む各種装置との関連で用いることができる。ディジタルカメラ２０は、マイクロプロセッサ制御部でのオペレーションでは、ディジタル画像をキャプチャリングし、ブロック２１内でアナログ電気信号に変換する電荷結合素子（ＣＣＤ）からなる画像センサを有する。次いでアナログ信号は処理ブロック２２（アナログ信号処理、Ａ／Ｄ変換を行う）で処理され、ディジタル化され、その後、ディジタル画像はフレームバッファ２３に一時的に記憶され、同時に処理ブロック２４（ディジタル画像変換処理を行う）でのディジタル処理に付される。

【００５７】処理ブロック２４はハードウェアまたはソフトウェアを用いて本発明の透かし挿入を行うが、フレームバッファ２３から入力される画像データは圧縮前のデータであるので、該データに対して伸張処理を行うことなくＤＣＴ変換し、透かし埋め込みを行う。処理ブロック２４は透かし埋め込み後の画像データをＪＰＥＧ等に圧縮し、ユーザ制御部のもとに、カメラ内蔵の画像記憶装置２６に記憶する。記憶ブロック（画像記憶装置２６）は、カメラ２０と取り外し可能型または固定型のいずれかのコンパクト磁気媒体または固体記憶媒体を有することができるし、また取り外し可能型の大容量ＰＣＭＣＩＡ仕様のハードディスクカードまたはフラッシュ記憶カードを含むことができる。

【００５８】カメラ２０は、それぞれアナログ出力部（Ｄ／Ａ変換およびアナログ出力を行う）２７およびディジタル出力部２８を含み、これらを通して画像データがカメラ内または外部装置に転送される。圧縮されない画像データはアナログ出力部２７を経由してカメラ２０内のＬＣＤスクリーン２９に転送されるか、またはＶＣＲやテレビ受像器のような外部装置に転送される。画像データは、圧縮であれ未圧縮であれ、ディジタル出力部２９を通してコンピュータシステムのようなディジタル装置にも転送され、ここで画像を表示したり、または透かし入り画像を検証することができる。

【００５９】図７は、ディジタル画像をキャプチャリング、処理、検証するために用いる各種コンポーネント間の相互関係を示すブロック図である。重要なコンポーネントの一つとしてコンピュータシステムがあり、図中では一般に符号３０で示す。コンピュータシステム３０は、メイ

ンフレームまたはパーソナルコンピュータのような適当な形式のものであってよい。

【００６０】コンピュータシステム３０は、慣用のマイクロプロセッサである中央処理装置（ＣＰＵ）３１、情報を一時的に記憶するランダムアクセスメモリ（ＲＡＭ）３２および情報を永久に記憶するリードオンリーメモリ（ＲＯＭ）３３からなる。これらの各コンポーネントはバス３４と接続している。コンピュータシステム３０のオペレーションは、典型的にはオペレーティングシステムのソフトウェアによって制御、調整される。システムメモリに組み込まれ、ＣＰＵ３１上で動作するオペレーティングシステムは、システム資源の配分を制御し、特に処理、メモリ管理、ネットワーキングおよびＩ／Ｏ機能のような種々のタスクを行うことによって、コンピュータシステム３０のオペレーションを行う。

【００６１】また、ディスケット３７のような不揮発性大容量記憶装置を挿入するディスケットドライブ３６はコントローラ３５によりバス３４と接続する。同様に、コントローラ３８は、バス３４とコンパクトディスク（ＣＤ）ＲＯＭ４０を受け入れるＣＤＲＯＭドライブ３９との間のインターフェースをとる。ハードディスク４１は、ディスクコントローラ４３によりバス３４と接続する固定ディスクドライブ４２の一部として設けられている。

【００６２】透かし挿入法のためのソフトウェアは、たとえばハードディスク４１に記憶され、実行に際してＣＰＵ３１に転送される。これとは別に、ソフトウェアをＲＡＭ３２またはＲＯＭ３３に記憶させてもよい。同様に、ディスケット３７およびＣＤＲＯＭ４０のような取り外し可能な記憶媒体装置を用いて、コンピュータシステム３０にディジタル画像データをロードしたり、またはシステムから抽出してもよい。

【００６３】ディジタル画像データはコンピュータシステム３０に入力されるが、別の方法であってもよい。フィルムカメラ４５で生成したフィルムベースの画像４４は記憶用のスキャナ４６によりディジタル化され、コンピュータ３０により処理される。ディジタルカメラ２０は上述の通り画像を直接ディジタル化し、これらをコンピュータ３０に転送することが可能である。コントローラ５３を経由してバス３４に接続するキーボード５１およびマウス５２はこのようなデータの入力を容易にするが、さもないと情報をコンピュータシステム３０に入力するための手段を用意することになる。

【００６４】また、遠隔配置を目的として、ディジタル画像データの転送をコンピュータ３０との間で行ってもよい。そのためには、コンピュータ３０は通信アダプタ５４を含むことができ、このアダプタにより直接接続またはモデム経由のローカルエリアネットワーク（ＬＡＮ）、インターネットまたはオンラインサービスを含むネットワーク５５との通信が可能になる。

【００６５】本発明によれば、例えばディジタルカメラ２０内で予め透かし入れしたディジタル画像を検証のためにコンピュータ３０に転送することができる。これとは別に、透かし無しのディジタル画像に透かしを入れ、そしてＣＰＵ３１で実行される適当なハードウェアまたはソフトウェアを用いて透かし入りディジタル画像をコンピュータ内で検証してもよい。

【００６６】コンピュータ３０内に転送または蓄積されたディジタル画像は多くの異なる方法で検証することができる。コンピュータ３０に付属するプリンタ５６はカラー印刷を行うが、その品質はプリンタ５６に依存して変動する。その他のオプションとして、コンピュータ３０に付属するディスプレイ５７上でのディジタル画像の検証がある。さらに別の手段としては、ＶＣＲを用いてテレビモニター上にディジタル画像を表示する方法もある。

【００６７】以上、特定の具体例により本発明を説明したが、当業者には明らかなように、さらに種々変更を加えることが可能である。例えば、本発明記載の目視可能な透かし挿入法は目視不能な透かし挿入法は、用途によっては組合せることができる。透かし挿入ステップで用いるブロックは用途次第で選択することができる。このように、本発明には特許請求の範囲の精神と範囲内に含まれるすべての変更が包含される。

【００６８】

【発明の効果】（１）改ざんを検出するための脆弱透かし方式を提供することができる。

【００６９】（２）ディジタル画像の周波数ドメインに直接インプリメントすることができるので、埋め込んだ透かしに起因する歪みを最小限に止める透かし挿入技術を提供することができる。

【００７０】（３）圧縮ディジタル画像の完全伸張を必須とせずに、挿入および検証の手順を行うことができる。

【００７１】（４）透かしを挿入したディジタル画像が改ざんを受けたか否かを検証することができる。ディジタル画像のための脆弱透かし挿入方式との関連で検証の手順を提供することができ、改ざんが発生したら、検証の手順が壊された透かしを明らかにでき、またそのディジタル画像の改ざん発生を知らせる基準を設けることもできる。

【００７２】（５）シークレットキーを挿入ステップでのみ用い、他方、検証は公開キーを用いて行う、周波数ドメイン透かしの挿入および検証を行うことができる。

【図面の簡単な説明】

【図１】本発明によるディジタル画像の周波数ドメインへの透かし挿入を示す一般的な概念図である。

【図２】本発明によるディジタル画像の周波数ドメインへの透かし挿入法に関連して初期の走査手順を示す流れ図である。

【図３】本発明によるディジタル画像の周波数ドメインへの透かし挿入法に関連してディジタル画像にビットを埋め込む手順を示す流れ図である。

【図４】本発明による、周波数ドメインにおける脆弱透かしの存在を透かしディジタル画像から検証することを示す概念図である。

【図５】ディジタル画像から透かしを抽出し、透かしの有効性を検証してディジタル画像が改ざんされたか否かを判断する方法示す流れ図である。

【図６】本発明との関連で用いるために取り付けたディジタルカメラのブロック図である。

【図７】本発明によるディジタル画像のキャプチャリング

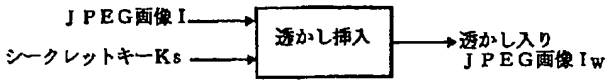
および検証、ならびにこのようなディジタル画像の処理に用いられる種々の成分間の相互関係を示すブロック図である。

【符号の説明】

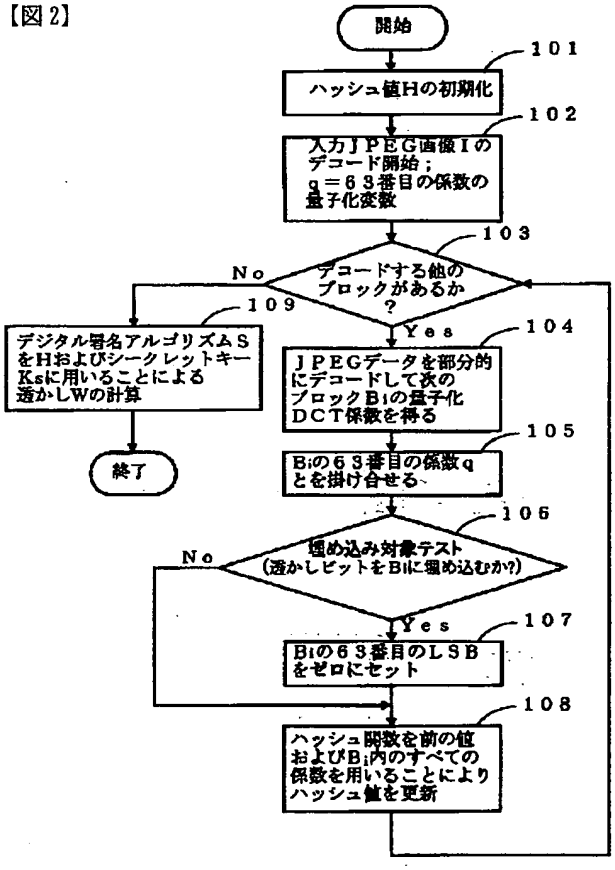
２０　ディジタルカメラ
２１　ＣＣＤディジタル画像センサ
２２　アナログ信号処理ブロック
２３　フレームバッファ
２４　ディジタル画像処理ブロック
２５　制御部
２６　インカメラディジタル画像記憶装置
２７　アナログ出力部
２８　ディジタル出力部
２９　ＬＣＤスクリーン
３０　コンピュータシステム
３１　ＣＰＵ
３２　ＲＡＭ
３３　ＲＯＭ
３４　バス
３５　コントローラ
３６　ディスケットドライブ
３７　ディスケット
３８　コントローラ
３９　ＣＤＲＯＭドライブ
４０　コンパクトディスク
４１　ハードディスク
４２　固定ディスクドライブ
４３　ディスクコントローラ
４４　フィルム
４５　フィルムカメラ
４６　スキャナ
５１　キーボード
５２　マウス
５３　コントローラ
５４　通信アダプタ
５５　ネットワーク
５６　プリンタ
５７　ディスプレイ

【図１】
【図２】
【図３】
【図４】
【図５】
【図６】
【図７】

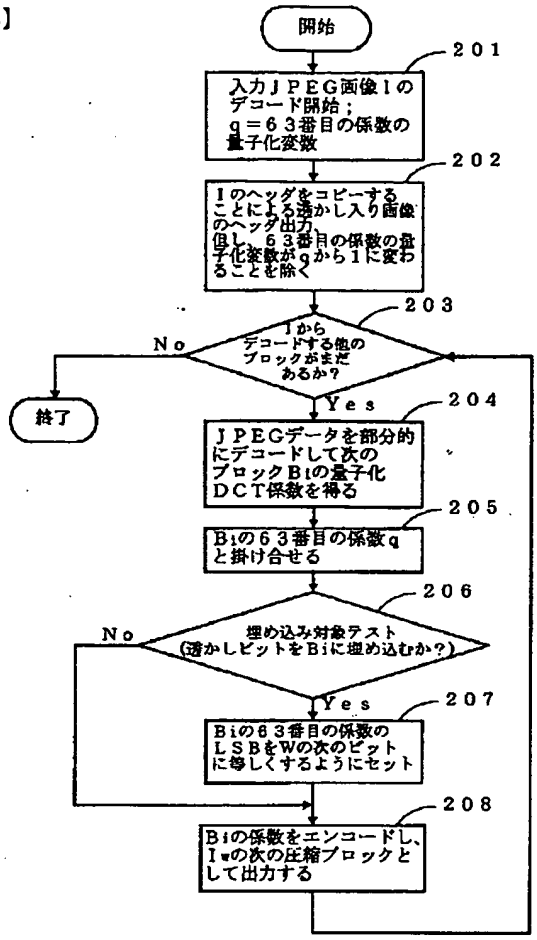
【図1】


ＪＰＥＧ画像Ｉ
シークレットキーＫｓ
透かし挿入
透かし入り
ＪＰＥＧ画像Ｉｗ

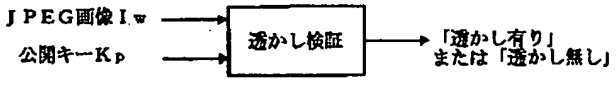
【図2】


開始
101
ハッシュ値Ｈの初期化
102
入力ＪＰＥＧ画像Ｉのデコード開始；ｑ＝６３番目の係数の量子化変数
103
デコードする他のブロックがあるか？
No
Yes
109
デジタル署名アルゴリズムＳをＨおよびシークレットキーＫｓに用いることによる透かしＷの計算
終了
104
ＪＰＥＧデータを部分的にデコードして次のブロックＢｉの量子化ＤＣＴ係数を得る
105
Ｂｉの６３番目の係数ｑとを掛け合せる
106
埋め込み対象テスト（透かしビットをＢｉに埋め込むか？）
No
Yes
107
Ｂｉの６３番目のＬＳＢをゼロにセット
108
ハッシュ関数を前の値およびＢｉ内のすべての係数を用いることによりハッシュ値を更新

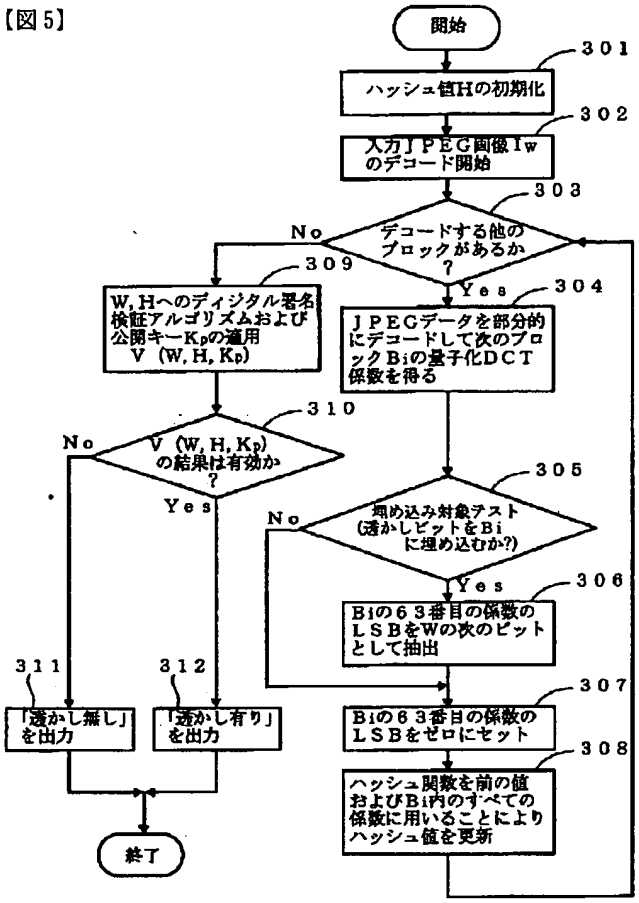
【図3】


開始
201
入力ＪＰＥＧ画像Ｉのデコード開始；ｑ＝６３番目の係数の量子化変数
202
Ｉのヘッダをコピーすることによる透かし入り画像のヘッダ出力（但し、６３番目の係数の量子化変数がｑから１に変わることを除く
203
Ｉからデコードする他のブロックがまだあるか？
No
Yes
終了
204
ＪＰＥＧデータを部分的にデコードして次のブロックＢｉの量子化ＤＣＴ係数を得る
205
Ｂｉの６３番目の係数ｑと掛け合せる
206
埋め込み対象テスト（透かしビットをＢｉに埋め込むか？）
No
Yes
207
Ｂｉの６３番目の係数のＬＳＢをＷの次のビットに等しくするようにセット
208
Ｂｉの係数をエンコードし、Ｉｗの次の圧縮ブロックとして出力する

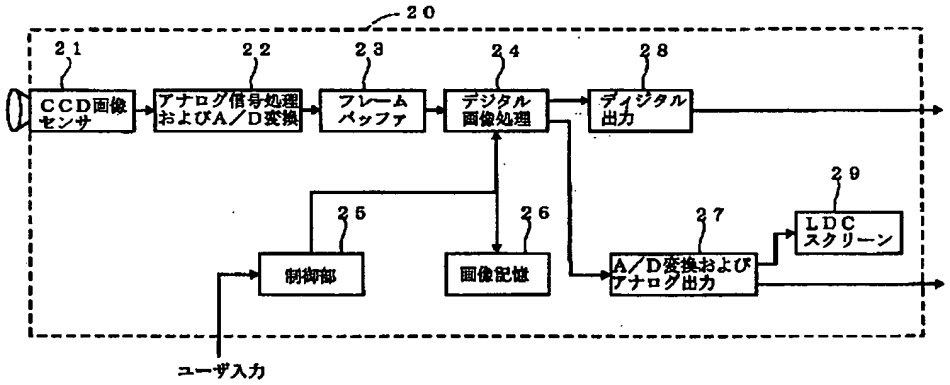
【図4】


ＪＰＥＧ画像Ｉｗ
公開キーＫｐ
透かし検証
「透かし有り」
または「透かし無し」

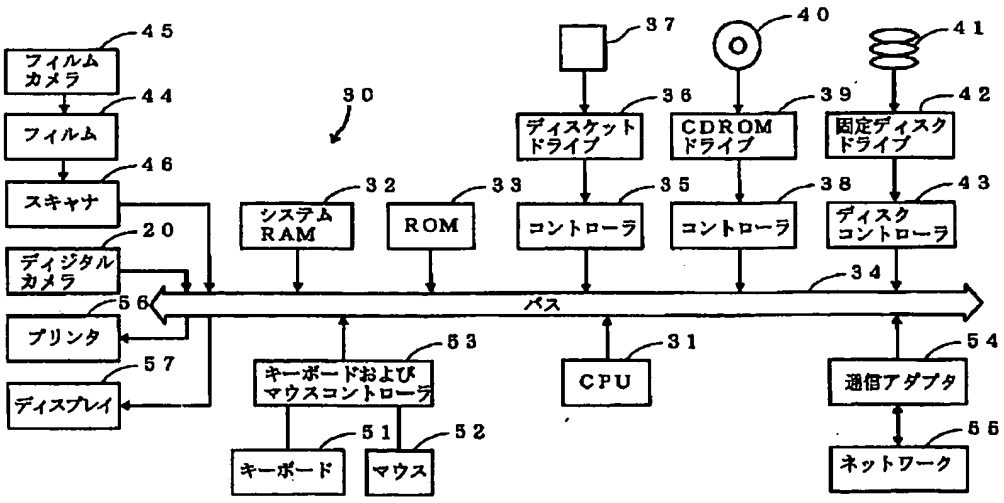
【図5】


開始
301
ハッシュ値Hの初期化
302
入力JPEG画像Iw
のデコード開始
303
デコードする他の
ブロックがあるか
?
No
Yes
309
W,Hへのディジタル署名
検証アルゴリズムおよび
公開キーKpの適用
V (W, H, Kp)
304
JPEGデータを部分的
にデコードして次のブロック
Biの量子化DCT
係数を得る
310
V (W, H, Kp)
の結果は有効か
?
No
Yes
305
埋め込み対象テスト
(透かしビットをBi
に埋め込むか?)
No
Yes
306
Biの63番目の係数の
LSBをWの次のビット
として抽出
311
312
「透かし無し」
を出力
「透かし有り」
を出力
307
Biの63番目の係数の
LSBをゼロにセット
308
ハッシュ関数を前の値
およびBi内のすべての
係数に用いることにより
ハッシュ値を更新
終了

【図6】


20
21
CCD画像
センサ
22
アナログ信号処理
およびA/D変換
23
フレーム
バッファ
24
デジタル
画像処理
28
ディジタル
出力
29
LDC
スクリーン
25
制御部
26
画像記憶
27
A/D変換および
アナログ出力
ユーザ入力

【図7】


45
フィルム
カメラ
44
フィルム
46
スキャナ
20
ディジタル
カメラ
56
プリンタ
57
ディスプレイ
30
37
ディスケット
ドライブ
40
CDROM
ドライブ
41
固定ディスク
ドライブ
36
39
42
32
システム
RAM
33
ROM
35
コントローラ
38
コントローラ
43
ディスク
コントローラ
34
バス
53
キーボードおよび
マウスコントローラ
31
CPU
54
通信アダプタ
51
キーボード
52
マウス
55
ネットワーク